CSS PLATINUM

Monthly Security Newsletter.

Welcome to the September edition:

We have been delighted to join our partners and customers at Cannes Yachting Festival!

For six days, over 600 exhibitors have been on display in the bay of Cannes, at the heart of the Cote d'Azur.

As well as over 650 boats and yachts on display, the festival is also showcasing a range of other products and services, with cyber security for superyachts and the maritime industry being a hot topic for discussion.

Looking forward to Monaco Boat Show!

Hot on the heels of Cannes will be the Monaco Boat Show begins on 28th September with a full schedule of events aimed at the new generation of yachting clients. Our CSS Platinum team looks forward to discussing all things cybersecurity with our clients and partners in Monaco!

CSS PLATINUM

Monthly Security Newsletter.

As featured in:

COMPASS IYBA

Aug / Sep 22

Cybercrime has evolved over the years and continues to increase as technology improves, with computing power getting more advanced and more affordable. The ubiquitous nature of technology in our lives, both in professional and personal settings, means we place a huge amount of trust in the devices we use each day.

Having our digital lives at our fingertips has allowed us to be more productive, saving time and effort. There are a number of potential drawbacks, however, because where there is data there is money to be made. Data is like gold to cyber criminals. In a digital world it is easy to gather, and more important, it can be anonymously monetized. There are many criminal- and state-sponsored actors (threat actors) who will target devices to extract the data contained within. Like many criminals they are opportunists and if they have no success initially, they will move on. It is important to make yourself and your vessel #hardtohack.

When it comes to cybercrime, these individuals and groups are highly indiscriminate and will target anyone who could easily be exploited or is vulnerable. No industry is exempt from this.

Click here to read full article.

THE LAW

CYBERSECURITY

The Importance of Staying Vigilant in a Growing Climate of Cybercrime

by **Doug Lucktaylor,** *CSS Platinum*

Cybercrime has evolved over the years and continues to increase as technology improves, with computing power getting more advanced and more affordable. The ubiquitous nature of technology in our lives, both in professional and personal settings, means we place a huge amount of trust in the devices we use each day.

Having our digital lives at our fingertips has allowed us to be more productive, saving time and effort. There are a number of potential drawbacks, however, because where there is data there is money to be made. Data is like gold to cyber criminals. In a digital world it is easy to gather, and more important, it can be anonymously monetized.

There are many criminal- and state-sponsored actors (threat actors) who will target devices to extract the data contained within. Like many criminals they are opportunists and if they have no success initially, they will move on. It is important to make yourself and your vessel #hardtohack.

When it comes to cybercrime, these individuals and groups are highly indiscriminate and will target anyone who could easily be exploited or is vulnerable. No industry is exempt from this.

Beware of ransomware

It a sad fact of life that a lot of people do not see the value of something until they no longer have access to it. This is often the case in ransomware attacks. Ransomware, once it has been released, will encrypt all the information on your device and make it inaccessible until you pay the attacker a significant fee to decrypt it. Unfortunately, there is no guarantee that he or she will release the data to you. The attacker also may sell the data to others, release it to the public or delete it even after you have paid.

There also have been occasions when a ransom was paid to release the data but nothing was done to protect against a subsequent attack, and the targets found themselves to be repeat victims of cybercrime. A well-defended network, protected devices and strong safety policies all will reduce the chance of these kinds of attacks from having a meaningful impact on your business.

The recreational marine industry is just as much of a target as any other industry. There is an ever-increasing reliance on technology for how vessels operate, including navigation, propulsion, entertainment, lighting and air conditioning systems, to name a few. In many cases these are controlled from one central management system, which puts them at high risk of exploitation.

It is therefore vital to have a robust risk-management process in place with a mitigation plan and defence strategy that everyone on your team understands and consistently helps to improve and maintain.

Where there is a computer network there will always be a threat from cyber attackers. Understanding the impact that each risk can have goes a long way in helping identify solutions to mitigate risk.

Cyber risk management

You may be aware of the IMO Resolution MSC.428(98), which states: "...a failure to demonstrate that cyber risks have been appropriately managed and IMO regulations adhered to, could result in refusal of the issue of a Document of Compliance." This is a requirement for any vessel that is greater than 500GT and subject to the IMO Code, but the risk of a cyber attack is present for vessels of any size and operation.

Where there is a computer network there will always be a threat from cyber attackers.

Your cyber resilience is an important part in a yacht protecting its guests, owners, crew and anyone they share data with. Brokers, suppliers, etc., all can be targets so everyone involved with the vessel at any level needs to be protected. Many organizations see cyber security as nice to have but do not see themselves as being at risk. As previously stated, anyone with data is a potential target for these cyber criminals. If you do not already have a cyber-risk management plan in place, consider partnering with a professional cyber security and data protection company. Don't become another statistic.

Doug Lucktaylor is head of information security at CSS Platinum, which provides IMO compliance auditing and a full suite of cyber security services to the superyacht industry. For more information, visit: cssplatinum.com.

Plan for the Autumn with a Superyacht Cybersecurity Audit

Assess and address security risks to ensure you are ready for your next flag audit.

Yacht Cyber Security Audit provides:

- Complete on-board evaluation
- Security Risk Assessment Report
- IMO Cyber Compliance Plan
- Incident Response Plan
- Workshop with Cyber Security Experts
- Risk Management Policies
- Cyber-Awareness Training

For further information contact the CSS Platinum team at support@cssplatinum.com